UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/611,809	07/07/2000	David K. Chin	BRCMP002	6867

7590 04/20/2006

CHRISTIE, PARKER & HALE
P.O. BOX 7068
PASADENA, CA 91109-7068

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 04/20/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/611,809	CHIN ET AL.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 February 2006* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,7-9,12 and 14-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,7-9,12 and 14-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 July 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 2/2/2006 has been entered.

Response to Arguments

1.1 In response to communications filed on 2/2/2006, applicant amends claim 1 and adds claims 28-29. The following claims 1-4, 7-9, 12, 14-29 are presented for examination.

1.2 Applicant's arguments, pages 7-11, filed on 2/2/2006, with respect to the rejection of claims 1-4, 7-9, 12, 14-27 have been fully considered, but they are not persuasive. Applicant argues "Hobson does not teach or suggest that a decode unit as claimed (e.g., "configured to determine if a square operation or a product operation needs to be performed on an operand) is "configured to issue the arithmetic instructions to the execution unit" where the execution unit is "configured to execute arithmetic instructions to perform product and square operations" as claimed. In Hobson instructions are only executed by the CPU. Instructions are not passed to the co-processor that performs the modular multiplication. Rather, the CPU "directly controls" the operation of the co-processor," Examiner respectfully disagrees. Hobson discloses known co-processor (figure 1 with detailed explanation in column 2) comprising multipliers and adders

configured to perform arithmetic instructions. Figure 6 with detailed explanation in column 6, lines 57 et seq. discloses "modular operation is performed in the co-processor without the intervention of the CPU" therefore, applicant's argument stating "In Hobson instructions are only executed by the CPU" is not correct. Applicant further argues that Hobson does not teach or suggest that the co-processor could or advantageously should receive instructions. Examiner respectfully disagrees. Hobson discloses a new co-processor that can reduce CPU overhead; "sequence of calculations may be done using a dedicated hardware state machine and arithmetic operations are available within the new co-processor namely addition and substraction", (see column 8, lines 4-42 and column 7, lines 60-65). Regarding Fisher, Applicant states, " FIG. 28 illustrates a circuit for the multiply-add instruction according to one embodiment of the invention. A control unit 240 processes the control signal for the multiply-add instruction. The control unit 240 outputs signals on an enable line 242 to control a packed multiply-adder 244. Fischer thus teaches that the decode unit executes the instructions. Fischer does not teach or suggest that the decode unit issues instructions to an execution unit that performs the multiply-add operation." Examiner respectfully disagrees. Applicant's interpretation of Fisher is not correct, the passage provided by Applicant states "the processor includes a decode unit, a set of registers, an execution unit, and internal bus for executing instructions" whereas Applicant alleges that the decode unit executes the instructions. It is inherent that an execution unit executes instructions and a decode unit decodes instructions to determine the operations to be performed by the execution unit. To provide further clarification and evidence that Applicant misinterprets the disclosure of Fisher, Examiner provides Applicant with prior art by the same assignee and common inventor Peleg that explicitly states that Execution unit is used to execute

operations and the decoder unit causes the execution unit to perform the required arithmetic instruction (see US Patent 6,385,634 to Peleg et al, column 7, lines 5-42 and figure 1). Therefore, Applicant has not overcome the rejection by amending the claims to include an execution unit configured to execute arithmetic instructions to perform product and square operations and the decode unit is configured to issue arithmetic instructions to the execution unit so that the execution unit performs specified multiplication and addition operations in parallel. Applicant argues "In response to Applicant's argument that the cited references do not teach or suggest performing multiplication and addition operations in parallel in a clock cycle as set forth, for example, in claims 23 and 24. The cited references teach performing the operations in multiple cycles. For example, Fischer teaches at column 6, lines 13 - 15 that a multiply-accumulate operation requires two instructions". Examiner asserts that Fisher discloses in column 7, lines 55-60 completing one or more of packed data instruction including multiple-add instruction in one clock cycle and further discloses complex multiplication to be performed in a single instruction such as multiply-substract instruction (see column 10, lines 28-30). Contrarily to applicant's argument, claims 23 and 24 do not claim performing multiplication and addition operations in parallel in a clock cycle as previously mentioned in the last Final office action. Upon further consideration, claims 1-4, 7-9, 12, and 14-29 still remain rejected in view of the prior art.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2.1 Claim 25 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claim 25, the addition of the word "type" to an otherwise definite expression extends the scope of the expression so as to render it indefinite. See MPEP § 2173.05(b).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3.1 **Claims 1-4, 5-6, and 9, 12, 14-27** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,209,016 to **Hobson et al.** in view of US Patent 6,237,016 to **Fisher et al.**

3.2 **As per claims 1, 2, 3, 21, and 22, Hobson et al.** substantially teaches an apparatus and method and a co-processor for performing modular multiplication and Montgomery algorithm comprising: an encryption processor (see figure 2) including: an execution unit configured to execute product and square operations, the execution unit including at least one adder and at least two multipliers (see figures 3-4). **Hobson et al.** discloses a decode unit in figure 6 that meets the recitation of a decode unit coupled to an instruction unit being configured to determine if a square operation or a product operation needs to be performed on an operand (see column 6, line 44 through column 7, line 23). **Hobson et al.** teaches performing multiplication and addition operations in parallel to improve performance time (see column 4, lines 27-40 and claim 7). **Hobson et al.** further suggests using instruction to control operations Hobson discloses a new co-processor that allows to act as a hardware engine capable of performing hardware instructions rather than under software control by the CPU thereby reducing CPU overhead; "sequence of calculations may be done using a dedicated hardware state machine and arithmetic operations are available within the new co-processor namely addition and substraction", (see column 7, line 60 through column 8, line 42). Although **Hobson et al** does not explicitly state that the decoder issues the arithmetic instructions to the co-processor, it is understood that the decoder makes the decision as to whether to perform a modular square or a modular multiply and by obviating the need for a CPU, arithmetic instructions are issued directly to the co-processor to the perform specific arithmetic instructions as the new co-processor now includes the arithmetic functions as cited and explained above (see column 6, line 44 through column 8, line 42). **Fisher et al** in an analogous art teaches a decode unit and execution unit for performing instructions and a decode unit issuing instructions to the execution unit to perform specific arithmetic operations (column

7, lines 23-33). Examiner's interpretation is clearly explained in ***US Patent 6,385,634 to Peleg et al, column 7, lines 5-42 and figure 1*** as mentioned above in the Response to Arguments, section 1.2. **Fisher et al** further discloses first instruction to perform simultaneous multiplication operations and second instruction to perform simultaneous multiplication-addition operations (see column 8, lines 12-41) one multiplication-addition operation can also be performed at one time in another embodiment (column 9, lines 6-8). **Fisher et al** adds that one of the advantages of this technique is to improve performance in performing complex calculations, for example Fisher discloses in column 7, lines 55-60 completing one or more of packed data instruction including multiple-add instruction in one clock cycle and further discloses complex multiplication to be performed in a single instruction such as multiply-substract instruction (see column 10, lines 28-30). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method of **Hobson** of determining whether to perform a Montgomery square operation or a Montgomery product operation in parallel and performing either the Montgomery square or Montgomery multiplication with the method of **Fisher et al** of issuing specific instruction to perform simultaneous multiplication operations and specific instruction to perform simultaneous multiplication and addition operations to provide a decoder unit issuing instructions comprising a first instruction to perform simultaneous multiplication operations and second instruction to perform simultaneous multiplication and addition operations in performing a square and an additional third instruction to perform simultaneous multiplication and addition operations in performing a multiplication as taught by **Fisher et al**. One skilled in the art would have been motivated by the suggestions provided by **Fisher et al** to make such a modification because performance of complex operations would

improve by performing calculations with fewer decoding instructions (column 9, lines 38-65 and column 10, lines 43-53).

As per claim 4, Hobson et al. discloses the limitation of wherein certain of the multiplication operations are performed in parallel using a multiply and shift (see column 2, lines 19-49). It is apparent to one skill in the art that certain of the multiplication operations can be processed in parallel as mentioned above by one instruction.

As per claim 5, Hobson et al. discloses the limitation of wherein the execution unit further comprises registers coupled to the multiplication units and the at least one adder (see figure 1).

As per claim 6, Hobson et al. discloses the limitation of wherein the encryption processor further comprises a memory coupled to the execution unit and the decode unit (see figure 6).

As per claim 12, Hobson et al. discloses the limitation of wherein the product and square operations executed by the execution unit are Montgomery product and square operations wherein the product and square operations are performed on operands (see column 1, lines 5-8 and column 2, lines 14-18).

As per claims 14-20, Hobson et al. substantially discloses a co-processor. It is known in the art hardware/software technologies that support encryption processor. Official notice is taken by examiner that it would have been obvious to have the encryption processor configured into a secure web server or a secure switch or internet load balance device deploying SSL/TLS or router or VPN gateways or remote access devices used for VPN applications. **Hobson et al.** does not disclose a secure switch deploying Secure Socket Layer (SSL)/Transport Layer Security (TLS). This modification would have been obvious because one skilled in the art would have been motivated to implement the encryption processor into the examples above to establish network security and take advantage of the processor speed in performing Montgomery calculation.

As per claims 23-25, the combination of **Hobson** and **Fisher et al** discloses an apparatus comprising of at least one adder and at least two multipliers (**Fisher et al**, column 9, lines 1-7) performing two specified multiplications in parallel using only one multiply-add instruction (**Fisher et al**, column 9, line 15 through column 10, line 53) that meets the recitation of at least one adder and at least two multipliers perform the specified multiplication operations in parallel in a first clock cycle. **Fisher et al** also suggests as alternative embodiment an apparatus capable of performing in one instruction multiply-add operation in combination with some other operation (column 10, lines 43-53). **Fisher** also discloses in column 7, lines 55-60 completing one or more of packed data instruction including multiple-add instruction in one clock cycle and further discloses complex multiplication to be performed in a single instruction such as multiply-substract instruction (see column 10, lines 28-30). Regarding the limitation of claim 25, as it is

known in the art for the processor to perform operations, instructions are given to the processor as to what operations need to be performed, therefore as indicated in both references specified instructions are given to perform specified functions (see **Fisher et al,** code examples in columns 23-26, claim 9 and column 7, lines 23-41 and column 16, lines 18-67). Examiner's interpretation is clearly explained in ***US Patent 6,385,634 to Peleg et al, column 7, lines 5-42 and column 13, lines 3-22, 45-48.*** Also a multiply-accumulate operation can perform multiplication operation and the result is added for an addition operation (column 15, lines 38-43). Alternative embodiment with different instruction name or different instructions and different combination of operations are within the scope of the teaching of Fisher (column 9, lines 60-67 and column 16, lines 56-58) as known in the art a multiplication and an addition operation can be performed in a single instruction similar to a calculator program. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the disclosure of **Hobson** of using apparatus or software control for controlling the sequence of operations as indicated in column 8, lines 1-41 and determining whether to perform a Montgomery square operation or a Montgomery product operation in parallel and performing either the Montgomery square or Montgomery multiplication with the method of **Fisher et al** of issuing specific instruction to perform simultaneous multiplication operations and specific instruction to perform simultaneous multiplication and addition operations to provide a decoder unit issuing instructions comprising a first instruction to perform simultaneous multiplication operations and second instruction to perform simultaneous multiplication and addition operations in performing a square and an additional third instruction to perform simultaneous multiplication and addition operations in performing a multiplication as taught by **Fisher et al**. One skilled in the art would

have been lead to make such a modification because the performance of complex operations such as Montgomery operations would improve by performing several calculations with fewer decoding instructions as suggested by **Fisher et al** (column 9, lines 38-45 and column 10, lines 43-53).

Claims 26-27 discloses similar limitation as found in claim 1, except for using modular operation; however, and the references also disclose operation to be performed on operand for a modular operation. Therefore, claims 26-27 are rejected on the same rationale as the rejection of claims 1 and 23-25.

As per claim 28, the combination of **Hobson et al and Fisher** discloses wherein the arithmetic instructions comprise a set of micro instructions (see **Hobson et al**, column 6, lines 57-67, column 7, lines 20-24; and column 8, lines 1-20) and (**Fisher**, column 7, line 40 through column 8, line 35).

As per claim 29, the combination of **Hobson et al and Fisher** discloses wherein the arithmetic instructions comprise a plurality of types of add-substract instructions and a plurality of types of multiply instructions (see **Hobson et al**, column 6, lines 57-67, column 7, lines 20-24; and column 8, lines 1-20) and (**Fisher**, column 7, line 40 through column 8, line 35).

4. **Claims 7-8** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,209,016 to **Hobson et al.** in view of US Patent 6,237,016 to **Fisher et al** as applied to claim 1 and further in view of US Patent 6,064,740 to **Curiger et al.**.

4.1 **As per claims 7 and 8, Hobson et al.** discloses the limitation of wherein the decode unit is further configured to decode an operation $M=C^d$ mod N and discloses determining whether to perform a square or multiply; and if the exponent d equals to a first logic state implement a square and a product operation. **Hobson et al.** does not explicitly teach the details of the process. However, **Curiger et al.** in an analogous art teaches (a) determining the MSB position of the exponent d equal to a first logic state and (b) issuing a first set of instructions to implement a square and a product operation after the MSB position of the exponent d equal to a first logic state is determined (see column 11, lines 3-9); (c) determining if the next most significant bit (MSB) of exponent (d) is the first digital state or a second digital state; and either (d) issuing a second set of instructions to the execution unit to implement a square operation if the next MSB is of the second digital state; or (e) issuing the first set of instructions to the execution unit if the next MSB of the exponent is of the first digital state instructions to implement a square and a product operation (see column 11, lines 9-15); and repeating (c) through (e) for every bit in the exponent (d) from the next MSB to the least significant bit (LSB) (see column 11, lines 15-25). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method and apparatus as combined above to apply the instructions as described above and the final result of the operation $M = C^d$ mod N by accumulating the results of (b) through (e) as taught by **Curiger et al.** to maximize the speed of the calculations. This

modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Curiger et al.** so as to maximize the speed of the calculations.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the art discloses performing multiplication operations in parallel and also performing multiplication and addition operations in parallel in one single instruction and further discloses configuring apparatus to perform specified operations in parallel.

US Patents: 3,665,411 O'Connor; 4,507,728 Sakamoto et al; 5,227,987 Imazawa et al

5,870,596 Yoshida.

5.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

cc

Carl Colin
Patent Examiner
April 15, 2006

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER